Solna 2021-12-20

Försvarsdepartementet

Er referens: Fö2021/00796
Vår referens: 21-012

Den 29:e september 2021 gick SOU 2021:63 “Sveriges säkerhet - behov av starkare skydd för nätverks- och informationssystem” (“utredningen”) ut på remiss. Här följer Netnods remissvar.

Inledningsvis anser Netnod den syn på certifiering som framkommer i utredningen övergripande är felaktig. Effekten av en väl genomförd certifiering blir inte bättre än kvalitet på de krav som certifieringen kontrollerar mot. Därför måste varje process som inkluderar certifiering börja med en kunskapsinsamling följt av omvandling av denna kunskap till kravställningar som i sin tur förankras hos de som ska certifieras. Först efter dessa steg som resulterat i krav av hög kvalitet kan och bör certifiering diskuteras. Det viktiga är att diskutera de krav som certifiering sker mot, och hur dessa tas fram, inte certifieringen i sig.

Detta inser Netnod är ett problem som grundar sig i att EU har denna enligt oss felaktiga syn på certifiering. Utredaren kan inte göra något åt detta. Dessutom ser Netnod i utredningen en övertro på certifiering av produkter, när istället en certifiering av processer som används för att designa, utveckla, införskaffa och driftsätta produkter kan leda till nog så hög effekt och detta utan att ha negativ påverkan på positiva marknadsmässiga krafter som konkurrens och innovation. Netnod anser därför den process som beskrivs som förslag i rutan i inledning av kapitel 12 är korrekt. Förutom detta förslag ser vi svagheter i hur utredaren ser på certifiering som verktyg för att uppnå önskad effekt.

Med det som bakgrund inkommer Netnod med synpunkter enligt bilaga.

Patrik Fältström
Teknik- och Säkerhetsskyddschef
Netnod

Bilaga 1

Sammanfattningsvis:

- **Definition av cybersäkerhet behövs**.
  Netnod anser att avsaknad av detta gör dokumentet svårgenomträngligt och förvirrande då begreppsotydligheten är påtaglig.
- **Säkerhet** kan ***ej*** uppnås genom central kontroll utan extremt goda kravställningar.
  Netnod anser att utredningen förbiser vikten av diversitet för ökad säkerhet.
- Termerna **informationssystem** samt **tillgång till informationssystem** är otydliga.
  Netnod anser att det måste förtydligas vad informationssystem innebär samt vad det innebär att ha tillgång till informationssystem, exempelvis i termer av tillgång till utvecklare, CI/CD-system, källkod, nyckelhanteringsprocesser och hårdvara.
- **Online och offline bör likställas.**
  Netnod anser att författningsförslaget ska förändras för att likställa online och offline, vilket är en nödvändighet i en digitaliserad värld.

Definition av cybersäkerhet

På s. 58 står det "*Det finns skäl för att begreppen – som utredningen tidigare framhållit i delbetänkandet – i största möjliga utsträckning bör ges samma betydelse när det tillämpas nationellt och internationellt, särskilt när det gäller det europeiska samarbetet*". Netnod anser inte att utredningen lever upp till att ge begreppen som används en likvärdig betydelse.

Utredningen använder begreppet cybersäkerhet i linje med hur IVA använder begreppet, vilket är att cybersäkerhet är en delmängd av begreppet IT-säkerhet med urvalskriteriet att det finns en antagonistisk aktör. ENISA använder däremot inte begreppet cybersäkerhet på samma sätt, utan använder cybersäkerhet (eng cybersecurity) även i de fall det saknas en antagonist.

Specifikt använder ENISA följande definitioner i Regulation 2019/881[1]:

> *'cybersecurity' means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats*
>
> *'cyber threat' means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons*

[1]2019/881 Title I, *Article 2,* Definitions, https://eur-lex.europa.eu/eli/reg/2019/881/oj/#d1e1148-15-1

Notera avsaknaden av nödvändig antagonist i ENISAs definitioner. Netnod anser att IVAs definition, dvs med antagonist, är den bättre av de två då den fokuserar på incidenter skapade av någon med en intention och att då är enklare att logisk skilja dessa från, exempelvis, naturkatastrofer.

Netnod vill även poängtera att incidenter och åtgärder inte är samma sak eller ens mappade ett-till-ett. Åtgärder som lindrar effekter av en cybersäkerhetsincident kan även hjälpa mot andra tänkbara incidenter. Åtgärden diversitet i ett kommunikationssystem lindrar konsekvenserna av både en cybersäkerhetsincident att en antagonist tar över en fastighet med kommunikationsutrustning och en incident att översvämning (en naturkatastrof) leder till bortfall av el.

Gällande begreppet “informationssystem” så anser utredningen att begreppet är väl utrett i tidigare arbeten, men utredningen refererar inte tydligt till vilken tolkning som utredningen använder sig av. Det resulterande lagförslaget måste vara applicerbart på faktisk verksamhet. Netnod anser förslagen i utredningen lutar ut att det ska vara enklare att sanktionera i efterhand än att göra rätt från början. Alla krav på produkter och tjänster måste i en marknadsekonomi vara kända i förväg för att ge en förutsägbarhet gällande begränsningar gällande innovation och produktutveckling.

Säkerhet kan *ej* endast uppnås genom central kontroll

Utredningen påstår att “*En tillräcklig informations- och cybersäkerhet kan **endast** uppnås när alla de olika förutsättningar som krävs för en sådan säkerhet är uppfyllda, dvs. enhetlig styrning och organisering av arbetet med informations- och cybersäkerhet, ett systematiskt informationssäkerhetsarbete i verksamheten och tekniska åtgärder samt tillsyn av efterlevnaden av regelsystem och ställda krav*“ (s. 23). Netnod anser inte att meningen är korrekt med ***endast***.

Idag består informationssystem av ett flertal olika ingående komponenter och funktioner. För ett sådant kan informations- och cybersäkerhet uppnås genom diversitet, redundans och koordinering mellan dessa ingående delar vilket resulterar i ett **minskat** behov av samordning mellan dem. Motsatsen är det som utredaren föreslår, ett centralt styrt och organiserat system.

Dessa två sätt kan ses som diametralt olika sätt att uppnå informations- och cybersäkerhet, där utredarens förslag, struktur och kontroll, kan ses som den naturliga vägen att gå där planering och utredning ligger före och är skilt från implementation. Framför allt i kontexten certifiering.

De stora vetenskapliga studier som gjorts på certifiering / legitimering och processer för dessa är hyfsat eniga om att den faktiska effekten av certifiering är förhållandevis liten jämfört med andra effekter, som utbildning eller marknadsincitament. Det finns inga vetenskapliga studier på certifiering av cybersäkerhetsprocesser, men det finns gott om studier kring till exempel

utbildning (det vetenskapliga område där flest studier kring effekter av certifiering görs), greenwashing och fairtrade. Dessa studier visar att certifieringen i sig ej är kvalitetsdrivande[2].

Det forskningen kommer fram till är snarare att certifiering är att se som en förändring av maktbalansen än en kvalitetshöjande åtgärd. Detta till en fördel av stora aktörer som har skalfördel för att bemöta certifieringskrav, allt annat lika[3].

Netnod vill därför poängtera att andra verktyg än certifiering kan användas för att uppnå god säkerhet, exempelvis god marknadsdesign, och att man bör närma sig certifiering försiktigt då certifiering kan få oanade marknadskonsekvenser till nackdel för vissa aktörskategorier, ofta mindre aktörer.

Vidare att när det kommer till faktisk implementation så är ett minskat behov av samordning och översyn att föredra då ökad översyn lätt leder till minskad diversitet.

Dessutom att det kan vara av hjälp att dela upp säkerhetsproblematiken i tre delar; tillgänglighet, riktighet och konfidentialitet, och att sedan utforma lagstiftning och kravställning därefter. Inklusive en anpassning av tillsyns- och andra kvalitetsprocesser (som krav vid, och uppföljning av, upphandling). Detta dels om ett delsystem som enbart tillhandahåller tillgänglighet och riktighet hamnar under en antagonists kontroll behöver inte detta nödvändigtvis leda till skada, och säkerligen inte leder till någon skada alls om systemet som helhet har diversifierat dessa funktioner. Netnod anser dessutom att vid explicit certifiering mot certifieringskrav är bättre med självcertifiering, dvs att man som leverantör hålls tills svars enligt marknadslogik av den som har köpt in en tjänst, alternativt av tillsynsmyndighet, snarare än att alla tjänster och produkter måste tredjepartscertifieras innan de blir tillgängliga på marknaden.

Netnod anser att säkerhet kan, speciellt relaterat till tillgänglighet, erbjudas genom diversifiering. Den övergripande principiella ståndpunkten Netnod har är att man kan minska konsekvenser av händelser på olika sätt (ex certifiering eller diversifiering) men att det är effekten av åtgärden som är det viktiga, inte åtgärden i sig. Ett problem med att enbart föreslå certifiering är att man

[2] Se speciellt Goldhaber & Brewer (2000) och Darling-Hammond, Berry & Thoreson (2001) som är två av de mest omfattande studierna i termer av bredd och tid på certifiering och konsekvenser. De noterar att certifiering i sig inte är kvalitetsdrivande, utan att andra faktorer, som lärarnas utbildning, spelar väsentligen större roll.

- Goldhaber, D. D., & Brewer, D. J. (2000). Does teacher certification matter? High school teacher certification status and student achievement. *Educational evaluation and policy analysis*, *22*(2), 129-145
- Darling-Hammond, L., Berry, B., & Thoreson, A. (2001). Does teacher certification matter? Evaluating the evidence. *Educational evaluation and policy analysis*, *23*(1), 57-77

[3] Se exempelvis Renard (2005) och hur fairtrade-certifieringen påverkar marknader och makt.

- Renard, M. C. (2005). Quality certification, regulation and power in fair trade. *Journal of rural studies*, *21*(4), 419-431.

minskar handlingsutrymmet för aktörer att själva välja lämpliga åtgärder. Innovation och produktutveckling måste kunna leda till nya effektivare åtgärder för att uppnå samma eller bättre effekt.

Online och offline ska likställas

Netnod är positiva till författningsförslaget då det likställer offline med online, dvs de myndigheter som har tillgång till, ex, lokaler under Säkerhetsskyddslagen ska också ha tillgång till digitala miljöer. Netnod vill dock poängtera att lydelserna för författningsförslagen i utredningen för Säkerhetsskyddslagen kapitel 3a inte är likvärdiga med de uppdaterade lydelserna för Säkerhetsskyddslagen (2018:585 uppdaterad enligt 2021:952) för kapitel 3a, dvs offline kommer inte helt likställas med online enligt nuvarande förslag.

Kapitel 3a använder genomgående samrådsmyndighet, medan Säkerhetsskyddslagen (2018:585 uppdaterad till 2021:952) har ändrat lydelserna till tillsynsmyndighet. Nedan följer Netnods förslag på ändringar.

Föreslagen lydelse i 2021:63	**Netnods förslag**
3 a kap 1 § tredje stycket Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med ***den myndighet som regeringen bestämmer (samrådsmyndigheten)***, innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras.	**3 a kap. 1 § tredje stycket** Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med ***tillsynsmyndigheten***, innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen konfidentiell eller högre tas i drift, eller i väsentliga avseenden förändras.
3 a kap. 2 § tredje stycket ***Samrådsmyndigheten*** får besluta att förelägga verksamhetsutövaren att vidta åtgärder enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.	**3 a kap. 2 § tredje stycket** ***Tillsynsmyndigheten*** får besluta att förelägga verksamhetsutövaren att vidta åtgärder enligt denna lag och föreskrifter som har meddelats i anslutning till lagen.
3 a kap. 3 § första stycket Om verksamhetsutövaren inte samråder med ***samrådsmyndigheten*** trots att det finns en skyldighet att göra det, får ***samrådsmyndigheten*** inleda samrådet.	**3 a kap 3 § första stycket** Om verksamhetsutövaren inte samråder med ***tillsynsmyndigheten*** trots att det finns en skyldighet att göra det, får ***tillsynsmyndigheten*** inleda samrådet.

Även i de föreslagna ändringarna i kapitel 7 och 8 finns det skillnader mot nuvarande lydelse i Säkerhetsskyddslagen (2018:585 med ändringar till 2021:952).

Föreslagen lydelse i SOU 2021:63	**Netnods förslag**
7 kap. 2 a § första stycket ***Samrådsmyndigheten*** får besluta att ta ut en sanktionsavgift av en verksamhetsutövare som 1. har åsidosatt sin skyldighet enligt 3 a kap. 2 § första och andra stycket, 2. har driftsatt eller förändrat ett informationssystem i strid med ett förbud som har meddelats med stöd av 3 a kap. 5 §, eller 3. har lämnat oriktiga uppgifter i samband med samråd enligt 3 a kap. 2 §.	**7 kap. 2 a § första stycket** ***Tillsynsmyndigheten*** får besluta att ta ut en sanktionsavgift av en verksamhetsutövare som 1. har åsidosatt sin skyldighet enligt 3 a kap. 2 § första och andra stycket, 2. har driftsatt eller förändrat ett informationssystem i strid med ett förbud som har meddelats med stöd av 3 a kap. 5 §, eller 3. har lämnat oriktiga uppgifter i samband med samråd enligt 3 a kap. 2 §.
7 kap. 9 § första stycket En sanktionsavgift ska betalas till ***samråds- eller*** tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.	**7 kap. 9 § första stycket** En sanktionsavgift ska betalas till tillsynsmyndigheten inom 30 dagar från det att beslutet om att ta ut avgiften har fått laga kraft eller inom den längre tid som anges i beslutet.
8 kap. 4 § första stycket Beslut om föreläggande enligt 3 a kap. 2 §, 4 kap. 9 och 15 §§ och 6 kap. 4 och 6 §§ eller sanktionsavgift enligt 7 kap. 1, 2 och 2 a §§ eller beslut om förbud enligt 3 a kap. 5 § får överklagas till Förvaltningsrätten i Stockholm. När ett sådant beslut överklagas är ***samråds- eller*** tillsynsmyndigheten motpart. Prövningstillstånd krävs vid överklagande till kammarrätten.	**8 kap. 4 § första stycket** Beslut om föreläggande enligt 3 a kap. 2 §, 4 kap. 9 och 15 §§ och 6 kap. 4 och 6 §§ eller sanktionsavgift enligt 7 kap. 1, 2 och 2 a §§ eller beslut om förbud enligt 3 a kap. 5 § får överklagas till Förvaltningsrätten i Stockholm. När ett sådant beslut överklagas är tillsynsmyndigheten motpart. Prövningstillstånd krävs vid överklagande till kammarrätten.

Lydelsen i nuvarande lag är att samrådan ska ske gällande säkerhetsklassifierade uppgifter i säkerhetsskyddsklassen *hemlig* eller högre, medan lydelsen för informationssystem är *konfidentiell* eller högre.

Föreslagen lydelse i SOU 2021:63	**2018:585**
3 a kap. 2 § första stycket	**4 kap. 9 § första stycket**
Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med den myndighet som regeringen bestämmer (samrådsmyndigheten), innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen ***konfidentiell*** eller högre tas i drift, eller i väsentliga avseenden förändras.	Om lämplighetsprövningen enligt 8 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren innan den inleder förfarandet samråda med tillsynsmyndigheten, om det planerade förfarandet innebär att den andra aktören kan få tillgång till 1) säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen ***hemlig*** eller högre, 2) eller annan säkerhetskänslig verksamhet av motsvarande betydelse för Sveriges säkerhet.

Netnod anser att kraven på samråd ska harmoniseras så att förfaranden som rör ***hemlig eller högre*** kräver samråd, så att inte informationssystem är under väsentligt skild lagstiftning från andra förfaranden (***hemlig*** vs ***konfidentiell***).

Netnod anser att lydelsen därför borde vara som följer:

Föreslagen lydelse i SOU 2021:63	**Netnods förslag**
3 a kap. 2 § första stycket	**3 a kap. 2 § första stycket**
Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren samråda med den myndighet som regeringen bestämmer (samrådsmyndigheten), innan ett informationssystem som kan förutses komma att behandla säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen ***konfidentiell*** eller högre tas i drift, eller i väsentliga avseenden förändras.	Om lämplighetsprövningen enligt 1 § leder till bedömningen att det planerade förfarandet inte är olämpligt från säkerhetsskyddssynpunkt, ska verksamhetsutövaren ***innan den inleder förfarandet*** samråda med tillsynsmyndigheten, innan ett informationssystem som kan förutses komma att behandla: ***1)*** säkerhetsskyddsklassificerade uppgifter i säkerhetsskyddsklassen ***hemlig*** eller högre, ***2) eller annan säkerhetskänslig information av motsvarande betydelse för Sveriges säkerhet.***

Tillgång till informationssystem

Netnod anser inte man kan använda begreppet ***informationssystem*** utan klargörande om vilka dimensioner det rör sig om. Det är oklart hur detta begrepp förhåller sig till andra begrepp som komponenter och moduler av informationssystem i en digital kontext? Netnod undrar om formuleringen "*tillgång till informationssystem"* (s. 48, författningsförslaget för 6 kap. 3 §) kan komma att tolkas som tillgång till digitala informationssystem **som användare**, snarare än fullständig tillgång till informationssystem och alla ingående delarna i dessa informationssystem (ex databaser, kodbaser, virtuella miljöer, containrar, krypteringsnycklar, CI/CD-miljöer, osv).

Notera att med stycket ovan vill Netnod poängtera att otydligheten kring informationssystem upplevs i flera dimensioner. Inte bara i dimensionen hårdvara - mjukvara och vilken tillgång man har till dessa under drift; utan även kring vilka processer som ligger till grund för informationssystemet som ska inkluderas (ex-ante och ex-post, en tidsdimension). Exempelvis är det, på en rent teknisk nivå, intressant för en aktör som vill få insyn i hur ett informationssystem används att även ha tillgång till hur ett informationssystem byggs (ex utvecklarmaskiner, processer för kodsigneringsnycklar, bygg-[4]containrar, uppsättning av paketeringsverktyg osv); speciellt i fallet då informationssystemet, eller dess klienter, uppdateras regelbundet och kanske till och med automatiskt.

Exempel på fall där hela bygg- och utvecklingsprocessen är intressant är de olika incidenter gällande supply chain som setts på sistone, tex Coop eller Maersk.

Säg att en leverantör levererar informationssystem med kundanpassningar till en myndighet som har verksamhet som faller under Säkerhetsskyddslagen. Hur kan tillsynsmyndigheter säkerställa att de som levererar systemet inte har medvetet lagt in bakdörrar (antagonistiskt hot som en del av cybersäkerhet) eller att de inte slarvar med hur de hanterar kodsigneringscertifikat eller nycklarna till dessa (ett IT-säkerhetshot)? Alternativt att en antagonist har lyckats påverka byggprocessen och injicerat bakdörrar. Om kodsigneringscertifikaten med nycklar kommer på vift är detta ett enormt säkerhetshot om det finns en CI/CD-pipeline uppsatt som en antagonist kan komma åt och potentiellt injicera sårbarheter i. Nuvarande formuleringar i utredningen visar inte på att utredaren till fullo förstått den komplexitet, och de potentiella attackvektorerna, som finns kring digitala system.

[4] *Bygg* betyder här processen där en mjukvaruapplikation skapas från källkod och andra ingående komponenter. En applikation som sedan används i produktion.

Netnod anser att på samma sätt som Säkerhetskyddslagen ger tillsynsmyndigheterna rätt att undersöka bygghandlingar för fastigheter (ex upphandlingsprocess, arkitekturritningar, detaljritningar, osv) såväl som faktiska fastigheter, borde Säkerhetsskyddslagen ge motsvarande rättigheter även i digitala fall, dvs för informationssystem.